Embedded PKI

The emerging state of the art

Asia PKI Forum 6th International Symposium
Chengdu, 27 July 2006

Stephen Wilson
Lockstep Consulting Pty Ltd, Australia

This presentation shows how contemporary PKI is moving towards embedded technologies, to dramatically streamline registration, improve usability, and simplify the supply of digital certificates.

To begin with, we review the fundamental benefits of PKI. There are many ways to perform electronic authentication. Many jurisdictions have technology neutral e-commerce laws and permit a range of different e-signature technologies. It is important therefore that we remember what makes digital signatures and PKI so special.

PKI's fundamental benefits

- Tamper resistant evidence of "who did what" in e-business; digital signatures easy to verify for many years
- Digital certificates convey *Authority Information* (e.g. credentials, licences, professional memberships etc.) as well as identity (or instead of identity)
- PKI smartcards are *"the only practical solution [to eavesdropping & account hijacking] today"*

  Bill Burr (NIST) Asia PKI Forum, Tokyo, Feb 2005
  http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf

Understanding evolves (1)

	Old PKI	New PKI
Meaning	"e-passport"	"e-business card"
Intended use	General purpose e-commerce	Specific applications
Certificates	Single one-size-fits-all certificate	Multiple certificates, increasingly embedded
Registration	Strict face-to-face ID proofing	Automatic for "known customers"

Understanding evolves (2)

Dr. Stephen Kent (co-chair IETF PKIX WG)

"For big CAs, there is an implicit assumption that a single cert. is all that a user should need. This assumes that one identity is sufficient for all applications, which contradicts experience."

Asia PKI Forum, Taipei, September 2005

Major trend in PKI today

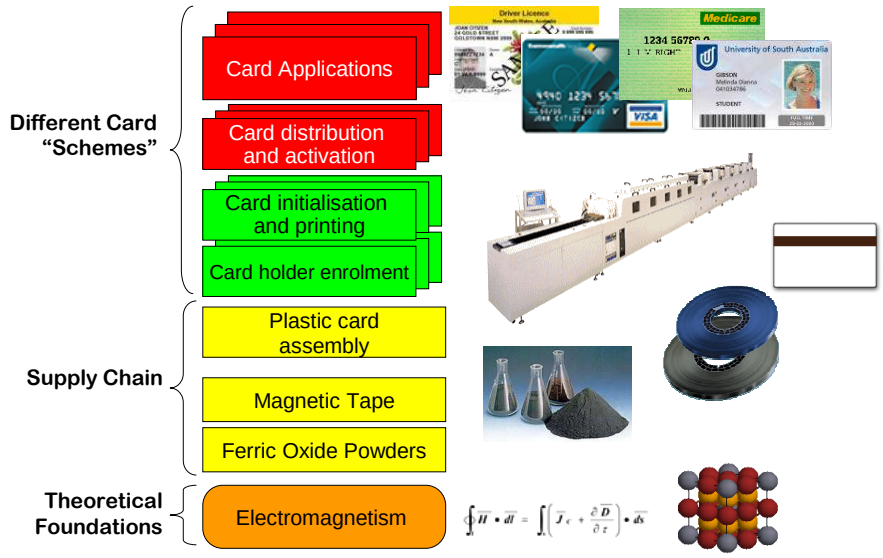
- **Different certificates for different domains (classes of applications)**
- **Multiple certificates**
- **Not hard to use if PKI is *embedded***

An important approach to simplifying PKI is to re-examine the "supply chain" for digital certificates, for two reasons:

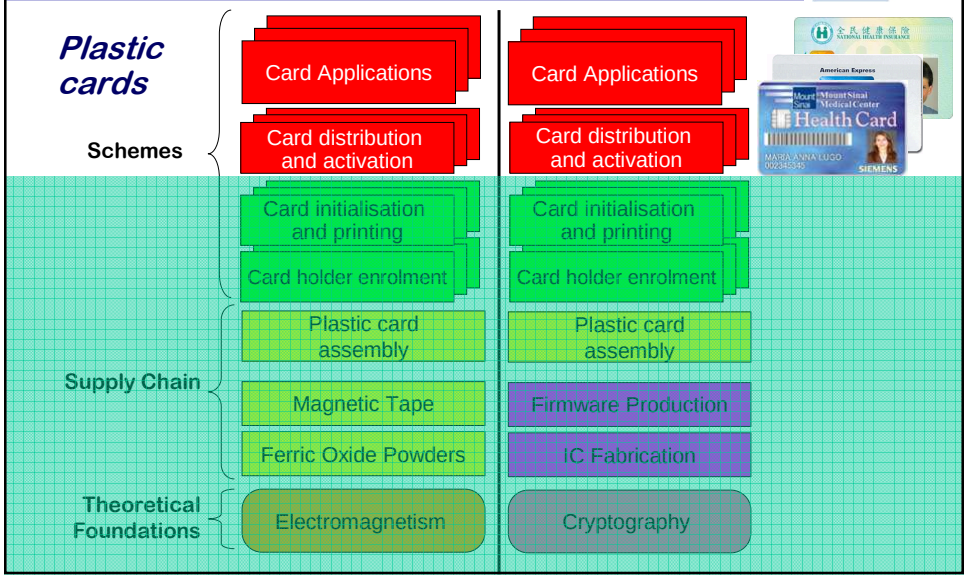
(1) Supply chain concepts show how different technological complexities can be separated and "buried" at different levels of the technology stack

(2) There is an instructive mature supply chain model metaphor in the plastic cards industry which shows the future of embedded PKI

Review: Plastic card technology stack



Ideal PKI technology stack



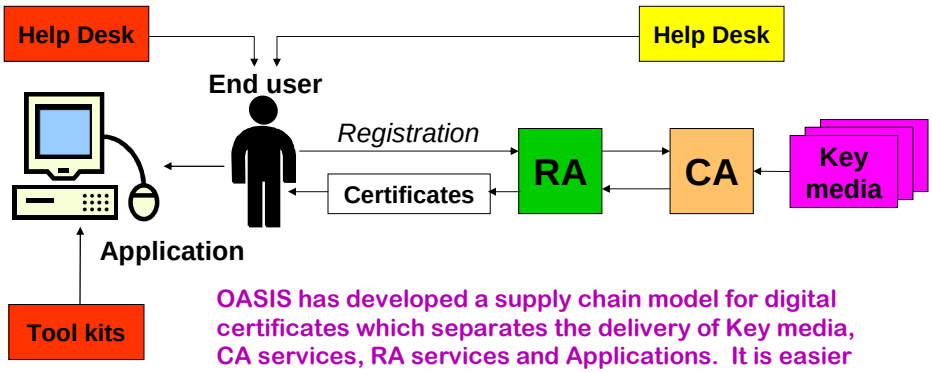
The comparison of technology stack and supply chains for magnetic stripe card and PKI smartcard provides the following lessons:

At the bottom levels, the technology stacks rest on very complex theoretical mathematics and physics.

Specialist manufacturers provide the lower level components (magnetic powders, and cryptographic firmware). Only a small number of specialist manufacturers are needed worldwide to support thousands of different schemes.

Users only see the "schemes"; they are unaware of complexities underneath. In particular, quite different supply chains for PKI and magnetic stripe cards lead to the same results at the scheme level.

OASIS Supply Chain Model



OASIS has developed a supply chain model for digital certificates which separates the delivery of Key media, CA services, RA services and Applications. It is easier to analyse ROI in this way, and it can encourage more flexible ways of supplying certificates. See also http://www.pkiforum.org/whitepaper/roi.pdf

Embedded PKI examples

Device authentication

Some of the oldest, most successful PKIs are for device authentication:

- **GSM SIM cards**
- **SSL server certificates**
- **IPsec VPN devices**
- ***Open Cable* TV set-top boxes**

Embedded PKI State of the Art

(1) Skype

- Each Skype subscriber receives a digital certificate embedded in Skype install
- "Zero User Interface" (ZUI) principle; i.e. Subscriber unaware they have a certificate!
- http://share.skype.com/sites/security

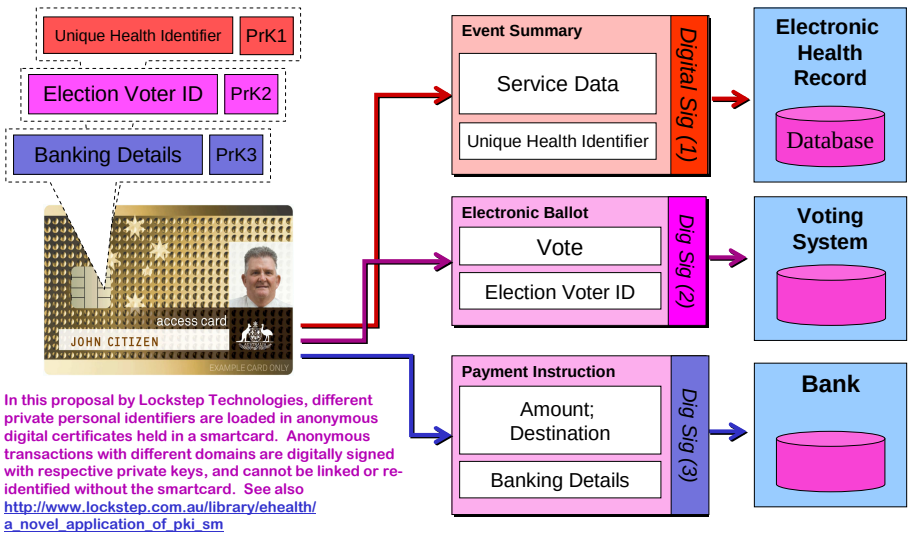
(2) Doctors' smartcards

- France (500,000)
- Chinese Taipei (300,000)
- Australia (10,000)
  - wide range of PKI enabled lodgments
  - electronic prescribing in development
  - "Known Customer" wholesale supply to hospitals etc.

(3) Fighting welfare fraud

- **Problem**
  - Some corrupt doctors create counterfeit Medicare (health insurance) claims for services not actually performed
- **Proposed solution**
  - Require all valid claims to be digitally signed using patient smartcard, as well as doctor smartcard
  - Each valid claim is then unique, and bound to a real patient
- **See also "Babysteps" No. 6 at** http://www.lockstep.com.au/library/babysteps

(4) Lockstep de-identification



In this proposal by Lockstep Technologies, different private personal identifiers are loaded in anonymous digital certificates held in a smartcard. Anonymous transactions with different domains are digitally signed with respective private keys, and cannot be linked or re-identified without the smartcard. See also http://www.lockstep.com.au/library/ehealth/a_novel_application_of_pki_sm

Policy implications

- **Digital certificates are not merely for identity; special purpose certificates will proliferate**
  Much PKI regulation is based on presumptions of general purpose electronic identity (and single certificates). Re-examination of policy and regulation may be needed in order to legitimise special purpose e-business card type certificates.
- **Expect to see small number of large volume "wholesale" CAs servicing many more RAs**
  If CA services are separated from RA services, then we could imagine a very small number of CAs offering bulk services worldwide, just as only a handful of specialist magnetic oxide powder suppliers exist worldwide. If the role of CA services is simplified to wholesale "minting" of different sorts of certificates, on order from RAs, then historical sovereignty issues disappear.
- **Cross recognition is much streamlined, at application / RA level**
  It is well known that cross recognition and interoperability is simpler at the "scheme level". A good example is credit card schemes which work seamlessly worldwide. In PKI, successful vertical cross border PKIs are appearing, e.g. Pan Asia Alliance.
- **Bridge CAs not the best interoperability model**
  The Bridge CA interoperability model is based on "Policy Mapping" between PKI domains, to establish equivalency. In the new PKI, each special purpose "e-business card" certificate has its own special meaning. Policy mapping is not relevant and the Bridge CA model is not applicable. Instead, the APEC Trust List model is probably more useful.
- **PKI becomes as easy to use as magnetic stripe cards!**

Further reading

Presentation available at www.lockstep.com.au

"Relationship Certificates"
www.lockstep.com.au/library/pki/relationship_certificates

"The Security Printer model for CA Operations"
www.lockstep.com.au/library/pki/the_security_printer_model_fo

Stephen Wilson
Lockstep Consulting
swilson@lockstep.com.au
+61 414 488 851